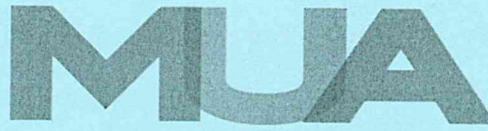


The
Management
University
of Africa



Sponsored by the Kenya Institute of Management

POST GRADUATE UNIVERSITY EXAMINATIONS

SCHOOL OF MANAGEMENT AND LEADERSHIP

DEGREE OF MASTER OF BUSINESS ADMINISTRATION

MBA 508: STRATEGIC MANAGEMENT INFORMATION SYSTEM

DATE: 9TH DECEMBER 2016

DURATION: 3 HOURS

MAXIMUM MARKS: 60

INSTRUCTIONS:

1. Write your registration number on the answer booklet.
2. **DO NOT** write on this question paper.
3. This paper contains **FOUR (4)** questions.
4. Question **ONE** is **compulsory**.
5. Answer any other **TWO** questions.
6. Question **ONE** carries **30 MARKS** and the rest carry **15 MARKS** each.
7. Write all your answers in the Examination answer booklet provided

QUESTION ONE

Read the Case Study below carefully and answer the questions that follow:

MONITORING EMPLOYEES ON NETWORKS

E-mail use has exploded as hundreds of millions of people the world over turn to it for speedy, convenient, and inexpensive business and personal communications. Not surprisingly, the use of e-mail for personal reasons at the workplace has also grown, as has use of the Web for personal business at work. A number of studies have concluded that at least 25 percent of employee online time is spent on non-work-related Web surfing, and perhaps as many as 90 percent of employees receive or send personal e-mail at work.

Many companies have begun monitoring their employees' use of e-mail and the Internet. A study by the American Management Association concluded that more than 75 percent of large U.S. companies are recording and reviewing employee communications and activities on the job, including e-mail, Internet connections, and computer files. Although U. S. companies have the legal right to monitor employee Internet and e-mail activity, is such monitoring unethical, or is it simply good business?

Managers worry about the loss of time and employee productivity when employees are focusing on personal rather than company business. If personal traffic on company networks is too high, it can also clog the company's network so that business work cannot be performed. Some employees at Xerox had sent so much junk and pornographic e-mail while on the job that the company's e-mail system shut down. Too much time on personal business, on the Internet or not, can mean lost revenue or overcharges to clients. Some employees may be charging time they spend trading their personal stocks online or pursuing other personal business to clients, thus overcharging the clients.

When employees use e-mail or the Web at employer facilities or with employer equipment, anything they do, including anything illegal, carries the company's name. Therefore, the employer can be traced and held liable. Management in many

firms fear that racist, sexually explicit, or other potentially offensive material accessed or traded by their employees could result in adverse publicity and even lawsuits for the firm. Even if the company is found not to be liable, responding to lawsuits could cost the company tens of thousands of dollars. Companies also fear e-mail leakage of trade secrets.

Companies have the legal right to monitor what employees are doing with company equipment during business hours. The question is whether electronic surveillance is an appropriate tool for maintaining an efficient and positive workplace. Some companies try to ban all personal activities on corporate networks—zero tolerance. Others block employee access to specific Web sites or limit personal time on the Web using software that enables IT departments to track the Web sites employees visit, the amount of time employees spend at these sites, and the files they download. Some firms have fired employees who have stepped out of bounds.

According to Steve Purdham, chief executive of Surf Control PLC, Congleton, England, a maker of content-filtering software, most companies primarily block access to sites dealing with pornography or illegal drugs. But a number also block access to Web sites dealing with sports, shopping, entertainment, and other distractions or limit access to certain times of the day, such as during lunch or after work hours.

Chaparral Energy, an Oklahoma City oil and gas producer, uses Websense software to block employee access to religious, political, and sexually oriented Web sites. It also bars Web-based e-mail sites and restricts online shopping to lunchtime and off-hours. After employees were informed their Internet use was being monitored, their time online fell from about an hour a day to less than 15 minutes per day.

Employee Web use for personal activities also fell at Comtech Telecommunications Corporation in Melville, New York after employees were informed they were being monitored. This satellite-communications company installed software that tracks individual users' surfing habits and provides managers with daily reports.

No solution is problem free, but many consultants believe companies should write corporate policies on employee e-mail and Internet use. The policies should include explicit ground rules that state, by position or level, under what circumstances employees can use company facilities for e-mail or Internet activities. The policies should also inform employees whether these activities are monitored and explain why.

The rules should be tailored to specific business needs and organizational cultures. For example, although some companies may exclude all employees from visiting sites that have explicit sexual material, law firm or hospital employees may require access to these sites. Investment firms will need to allow many of their employees access to other investment sites. A company dependent on widespread information sharing, innovation, and independence could very well find that monitoring creates more problems than it solves.

Required

- a) Evaluate the role of information systems in supporting various levels of Business strategy (6 Marks)
- b) Using relevant examples explain why managers should monitor employee e-mail and Internet usage (6 Marks)
- c) Describe an effective email and Web use policy for a company (8 Marks)
- d) Describe Five characteristics of Decision Support System (10 Marks)

QUESTION TWO

- a) Describe Five goals of information security (5 Marks)
- b) By using suitable examples differentiate between tacit and explicit knowledge (4 Marks)
- c) Using relevant examples differentiate between strategy and strategic information system (6 Marks)

QUESTION THREE

- a) Describe how knowledge has a location (4 Marks)
- b) Explain Four factors to be considered when purchasing hardware (4 Marks)
- c) Briefly explain Seven threats to computerized information system (7 Marks)

QUESTION FOUR

- a) Describe how information systems are transforming organizations today
(5 Marks)
- b) Using Competitive Forces Models explain five competitive strategies that a firm can use to deal with these competitive forces.
(10 Marks)

